REMARKS

The claims remaining in the present application are Claims 1-27. The Examiner is thanked for performing a thorough search. Claims 1, 12, and 16 have been amended. Support for the amendment to Claim 1 can be found in the instant application 10/627,374 in the description of step 150, for example, from the bottom of page 13 to the end of the first paragraph on page 14. Support for the amendment to Claim 12 can be found in Claims 14 and 15.

CLAIM REJECTIONS

35 U.S.C. §102

Claims 1, 3-4, 6-9, 12-27

Claims 1, 3, 4, 6-9, 12-27 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,578,147 by Shanklin et al. (referred to hereinafter as "Shanklin"). Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Shanklin.

> Amended independent Claim 1 recites,
>
> A method for configuring an intrusion detection system in a network, comprising:
>
> determining a location for a deployed intrusion detection sensor of said intrusion detection system wherein said sensor in enabled to monitor communication in a portion of said network;
>
> deploying said intrusion detection sensor in said location in said network;
>
> tuning said intrusion detection sensor to an appropriate level of awareness of content in said communication in said network so that an appropriate response can be generated based on a type of a detected intrusion in said network;
>
> prioritizing responses generated by said intrusion detection sensor to achieve said appropriate response to said detected intrusion in said network, wherein said prioritizing is based on said type of said detected intrusion; and
>
> configuring intrusion response mechanisms in said network so that said mechanisms provide said appropriate response to said detected intrusion.

Applicants respectfully submit that Shanklin does not teach or suggest, among other things, "tuning said intrusion detection sensor to an appropriate level of awareness of content in said communication in said network so that an appropriate response can be generated based on a type of a detected intrusion in said network; prioritizing responses generated by said intrusion detection sensor to achieve said appropriate response to said detected intrusion in said network, wherein said prioritizing is based on said type of said detected intrusion; and configuring intrusion response mechanisms in said network so that said mechanisms provide said appropriate response to said detected intrusion," as recited by Claim 1.

Shanklin teaches parallel intrusion detection sensors with load balancing for high speed networks. As Col. 2 lines 48-50, Shanklin states that "Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'internetworking device' such as a router or a switch." Shanklin goes on to state at Col. 2 lines 62-67, "...each sensor is identical to the other sensors and is capable of performing the same intrusion detection processing. The sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a 'signature' that matches one of a collection of known intrusion signatures" (emphasis added). Since Shanklin teaches that "each sensor is identical to the other sensors" Shanklin teaches away from , among other things, "tuning said intrusion detection sensor..." as recited by Claim 1.

The Office Action asserts that Shanklin teaches "tuning said intrusion detection sensor to an appropriate level of awareness of content in said communication in said network so that an appropriate response can be generated based on a type of a detected intrusion in said network" at Col. 3 lines 55-65. Col. 3 lines 64-65 state, "...sensor 11 may have appropriate functionality so that if it detects an intrusion, it can take appropriate action, such as terminating the connection." However, having functionality to take appropriate action does not teach any kind of "tuning" let alone teach "tuning said intrusion detection sensor to an appropriate level of awareness of content in said communication in said network so that an appropriate response can be generated based on a type of a detected intrusion in said network."

The Office Action asserts that Shanklin teaches "prioritizing responses generated by said intrusion detection sensor to achieve said appropriate response to said detected intrusion in said network, wherein said prioritizing is based on said type of said detected intrusion... configuring intrusion response mechanisms in said network so that said mechanisms provide said appropriate response to said detected intrusion" at Col. 4 lines 54-67. Shanklin teaches at Col. 4 lines 54-67 analyzing packets, having the sensor take action, and using known network service vulnerabilities to inspect packet headers. However, no where does Col. 4 lines 54-

67 teach "prioritizing responses…" let alone teach "prioritizing responses generated by said intrusion detection sensor to achieve said appropriate response to said detected intrusion in said network, wherein said prioritizing is based on said type of said detected intrusion" (emphasis added). Further, no where does Col. 4 lines 54-67 teach "configuring intrusion response mechanisms…" let alone teach "configuring intrusion response mechanisms in said network so that said mechanisms provide said appropriate response to said detected intrusion." For the foregoing reasons, Claim 1 should be patentable.

Amended independent Claim 12 recites,

> A system for protecting security of a provisionable network comprising:
> a network server;
> a pool of resources coupled with said server for employment by a client;
> a resource management system for managing said resources; and
> an intrusion detection system enabled to detect and respond to an intrusion in said network, wherein said intrusion detection system comprises an intrusion detection sensor that is tunable to determine a threat level posed by a detected intrusion.

As already stated, Shanklin does not teach an intrusion detection sensor that is tunable. Therefore, Shanklin does not teach or suggest "wherein said intrusion detection system comprises an intrusion detection sensor that is tunable to determine a threat level posed by a detected intrusion," (emphasis added) as recited by Claim 12. For the foregoing reasons, Claim 1 should be patentable.

Independent Claim 19 recites,

> A network intrusion detection system, comprising:
> a network device comprising intrusion detection software, said device communicatively coupled with a provisionable network;
> a trust hierarchy, comprising a portion of said network and enabled to communicate with said software and to cause evaluation of a detected intrusion;
> a deployable, tunable, intrusion detection sensor; and
> a network device enabled to generate a response to a detected intrusion

As already stated, Shanklin does not teach an intrusion detection sensor that is tunable. Therefore, Shanklin cannot teach "a deployable, tunable, intrusion detection sensor," as recited by Claim 19.

Claims 3, 4, 6-9 depend on Claim 1. Claims 13-18 depend on Claim 12. Claims 20-27 depend on Claim 19. These dependent claims include all of the limitations of their respective independent claims. Further, these dependent claims include additional limitations which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

CONCLUSION

In light of the above listed amendments and remarks, reconsideration of the rejected claims is requested. Based on the arguments and amendments presented above, it is respectfully submitted that Claims 1-27 overcome the rejections of record. For reasons discussed herein, Applicant respectfully requests that Claims 1-27 be considered be the Examiner. Therefore, allowance of Claims 1-27 is respectfully solicited.

Should the Examiner have a question regarding the instant amendment and response, the Applicant invites the Examiner to contact the Applicant's undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER, MURABITO & HAO LLP

Dated: 1/17/, 2007

John P. Wagner Jr.
Registration No. 35,398

Address:

Westridge Business Park
123 Westridge Drive
Watsonville, California 95076 USA

Telephone:

(408) 938-9060 Voice
(408) 234-3749 Direct/Cell
(408) 763-2895 Facsimile